

**ISLE OF MAN  
FINANCIAL SERVICES AUTHORITY**

---

*Lught-Reill Shirveishyn Argidoil Ellan Vannin*

**Anti-Money Laundering and Countering  
the Financing of Terrorism  
Supplemental Information Document  
July 2021**

Whilst this publication has been prepared by the Financial Services Authority, it is not a legal document and should not be relied upon in respect of points of law. Reference for that purpose should be made to the appropriate statutory provisions.

## Contents

1. Introductory .....	3
2. General requirements and risk based approach .....	4
3. Customer due diligence, ongoing monitoring and enhanced measures.....	4
3.1 Introduced business scenarios .....	4
3.1.1 Scenario 1.....	4
3.1.2 Scenario 2.....	7
3.1.3 Scenario 3.....	9
3.1.4 Scenario 4.....	11
3.1.5 Scenario 5.....	13
3.2 What information to verify .....	15
3.2.1 Natural persons.....	15
3.2.2 Legal arrangements .....	15
3.2.3 Foundations .....	16
3.2.4 Legal persons .....	16
3.3 Examples of methods to verify identity and address.....	16
3.3.1 Example methods to verify the identity of a natural person .....	16
3.3.2 Example methods to verify a natural person’s address .....	17
3.3.3 Example methods to verify legal arrangements.....	19
3.3.4 Example methods to verify foundations.....	19
3.3.5 Example methods to verify legal persons.....	20
3.3.6 Example methods for verifying the natural persons with the power to direct a customer .....	20
3.4 Certification of hard copy documents .....	20
3.5 Electronic methods to verify identity and address .....	21
3.6 Methods for meeting a customer .....	23
4. Exemptions and simplified measures .....	24
5. Reporting and registers.....	24
6. Compliance and record keeping .....	24
7. Miscellaneous .....	25

## 1. Introductory

The purpose of the Supplemental Information Document is to provide further information to relevant persons supervised or overseen for Anti-Money Laundering and Countering the Financing of Terrorism (“AML/CFT”) purposes by the [Isle of Man Financial Services Authority](#) (“the Authority”). Relevant persons must understand and satisfy their obligations under the Anti-Money Laundering and Countering the Financing of Terrorism Code 2019 (“the Code”). The Code can be found at the Isle of Man Government’s [legislation website](#). Guidance in relation to the Code can be found in the [Anti-Money Laundering and Countering the Financing of Terrorism Handbook](#) (“the Handbook”). Guidance in relation to specific sectors can be found in the [sector specific AML/CFT guidance notes](#). The information contained in the Supplemental Information document does not have the status of guidance nor is it legislation or legal advice.

This Supplemental Information Document is not exhaustive, and does not create any requirements or a checklist which must be followed. Where lists or examples are provided they are for information only, and offered to assist relevant persons in considering how they may meet their AML/CFT obligations. Each relevant person must consider its own particular circumstances on a reasonable risk basis and consider what they can do to prevent or mitigate the risks of Money Laundering and the Financing of Terrorism (“ML/FT”). This includes additional measures and controls that it may be necessary to implement in order to prevent its exploitation, and that of its products and services, by persons seeking to launder criminal property or to finance terrorism or the proliferation of weapons of mass destruction.

For ease of reference, the Supplemental Information Document contains extracts from relevant legislation which are boxed for clarity. However, these extracts must not be considered as a substitute for the original documents. All Isle of Man primary legislation can be found [here](#) and all Isle of Man secondary legislation can be found [here](#). The Supplemental Information Document follows the order of the Handbook.

If a term is defined in the Code the same definition applies in the Supplemental Information Document. All abbreviations used in the Supplemental Information Document, which are not otherwise used in the Code, are expanded in the Supplemental Information Document’s glossary. Should any inconsistencies occur between the text in the Supplemental Information Document and the Code, the Code has primacy.

Relevant persons must note that where the term “financing of terrorism” or its abbreviation “FT” are used, they also include “the financing of proliferation” (“FP”). Accordingly where “countering the financing of terrorism” or “CFT” are used, they also include “countering the financing of proliferation” (“CFP”).

The Supplemental Information Document is not the only additional source of information on ML/FT risks or on meeting AML/CFT obligations. Other sources include:

- the [AML/CFT Handbook](#);
- [sector specific guidance](#) published by the Authority;
- the Isle of Man's [National Risk Assessment](#) published by the Cabinet Office;
- guidance and good practice provided by the [IOMFIU](#) on making suspicious activity reports;
- guidance issued by the [IOMCE](#) on Financial Sanctions, Terrorism and Terrorist Financing, Proliferation and Proliferation Financing and Trade Based Money Laundering;
- guidance issued by the [Financial Action Task Force](#) ("FATF") on ML/FT risk;
- guidelines on AML/CFT matters including on customer due diligence ("CDD") issued by the [Bank for International Settlements Basel Committee on Banking Supervision](#); and
- guidelines on risk factors issued by the [European Supervisory Authorities](#).

## 2. General requirements and risk based approach

There is no supplemental information associated with this chapter of the Handbook.

## 3. Customer due diligence, ongoing monitoring and enhanced measures

### 3.1 Introduced business scenarios

<sup>Code 9</sup> Below are some example scenarios written to aid with interpretation of paragraphs 9(6) and (7). Whilst these scenarios have been written using specific sectors, the circumstance described are applicable to all sectors.

#### 3.1.1 Scenario 1

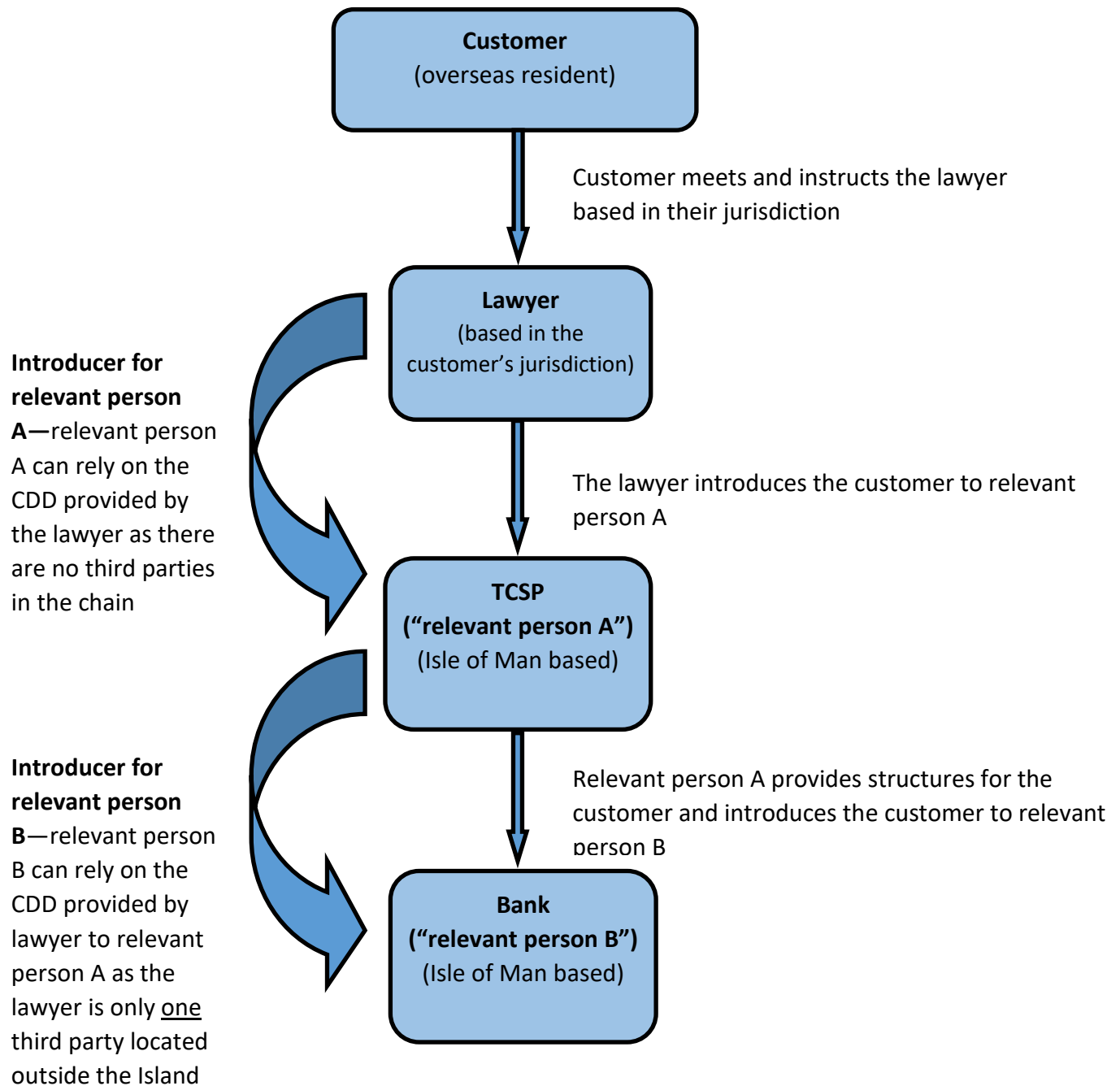
A customer who is an overseas resident meets and instructs a law firm based in their jurisdiction, which then introduces the customer to an Isle of Man TCSP (*relevant person A*). The Isle of Man TCSP provides structures for the customer and in the course of this introduces the customer to an Isle of Man bank (*relevant person B*).

The Isle of Man based businesses rely on CDD and evidence of verification of identity provided by the law firm. In this scenario the law firm is the introducer to relevant person A and there are no third parties in the chain.

For relevant person B, the introducer is relevant person A and the law firm is a third party being the only third party in the process located outside the Island.

Both the TCSP and the bank are therefore able to rely on the evidence of verification of identity provided by the law firm and are not required to obtain this again through other means (i.e. the provisions of paragraphs 9(6) and (7) do not apply).

**Scenario 1**



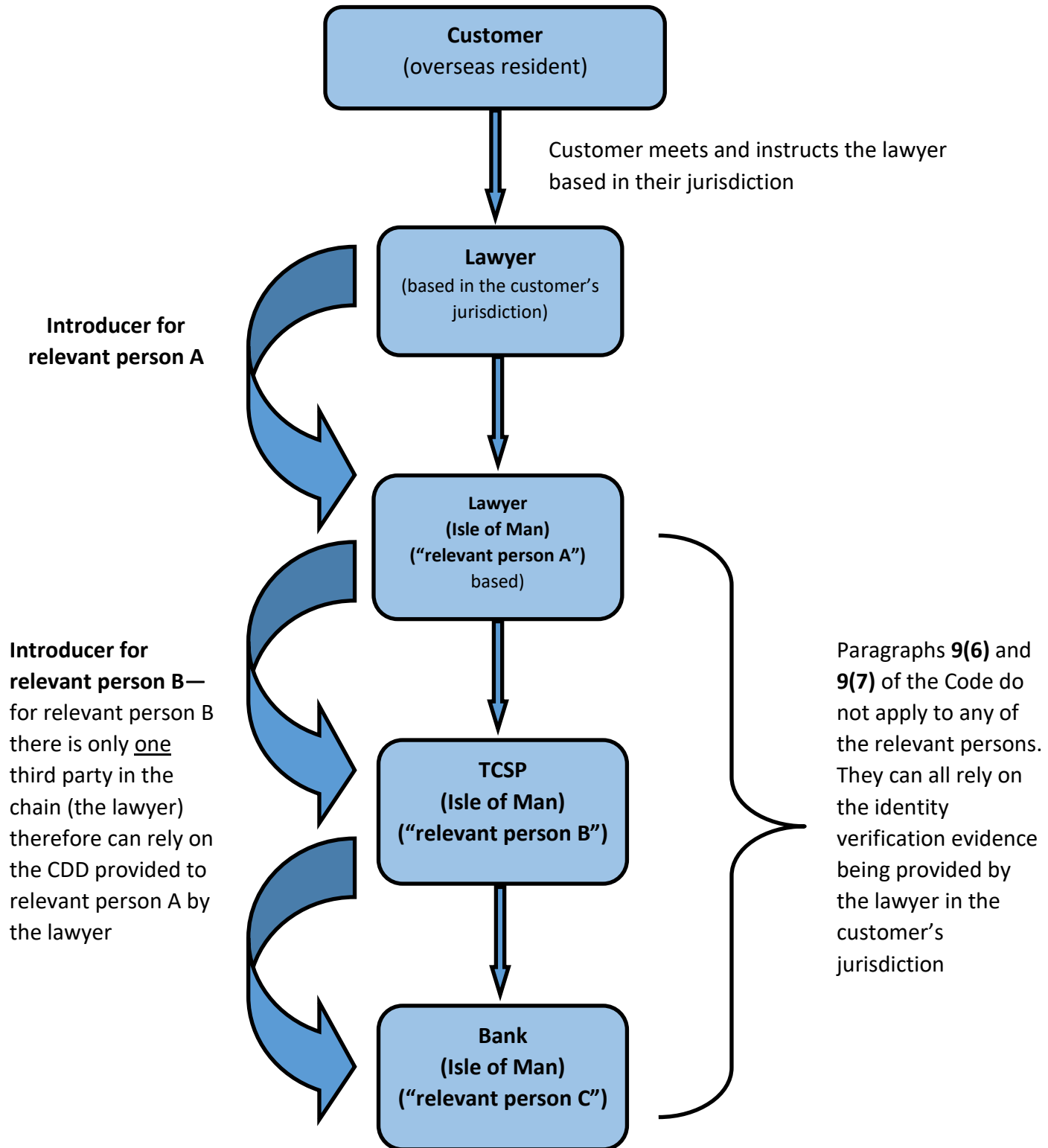
### 3.1.2 Scenario 2

A customer who is an overseas resident instructs a law firm based in their jurisdiction who then introduces the customer to an Isle of Man law firm (*relevant person A*). The Isle of Man law firm then introduces the customer to an Isle of Man TCSP (*relevant person B*) which then introduces the customer to an Isle of Man bank (*relevant person C*). As in the previous example, all three Isle of Man businesses rely on CDD and evidence of verification of identity provided by the overseas law firm.

In this scenario the law firm is the introducer to relevant person A and there are no third parties in the chain. In addition, relevant person A is the introducer to relevant person B, which is itself the introducer to relevant person C. As far as relevant person B is concerned there is only one third party in the chain, the overseas law firm, so it can rely on the evidence of verification of identity provided by that entity (i.e. the provisions of sub paragraphs (6) and (7) do not apply).

For relevant person C there are two third parties involved in the process (Isle of Man law firm, and the overseas law firm), but only one is located outside the Island so it too can rely on evidence of verification of identity provided through the chain (i.e. the provisions of sub paragraphs (6) and (7) do not apply).

Scenario 2





### 3.1.3 Scenario 3

A customer who is an overseas resident instructs a law firm based in their jurisdiction (law firm A) which introduces the customer to another law firm located in a different overseas jurisdiction (law firm B). Law firm B introduces the customer to an Isle of Man TCSP (relevant person A) which in turn introduces the customer to an Isle of Man bank (relevant person B).

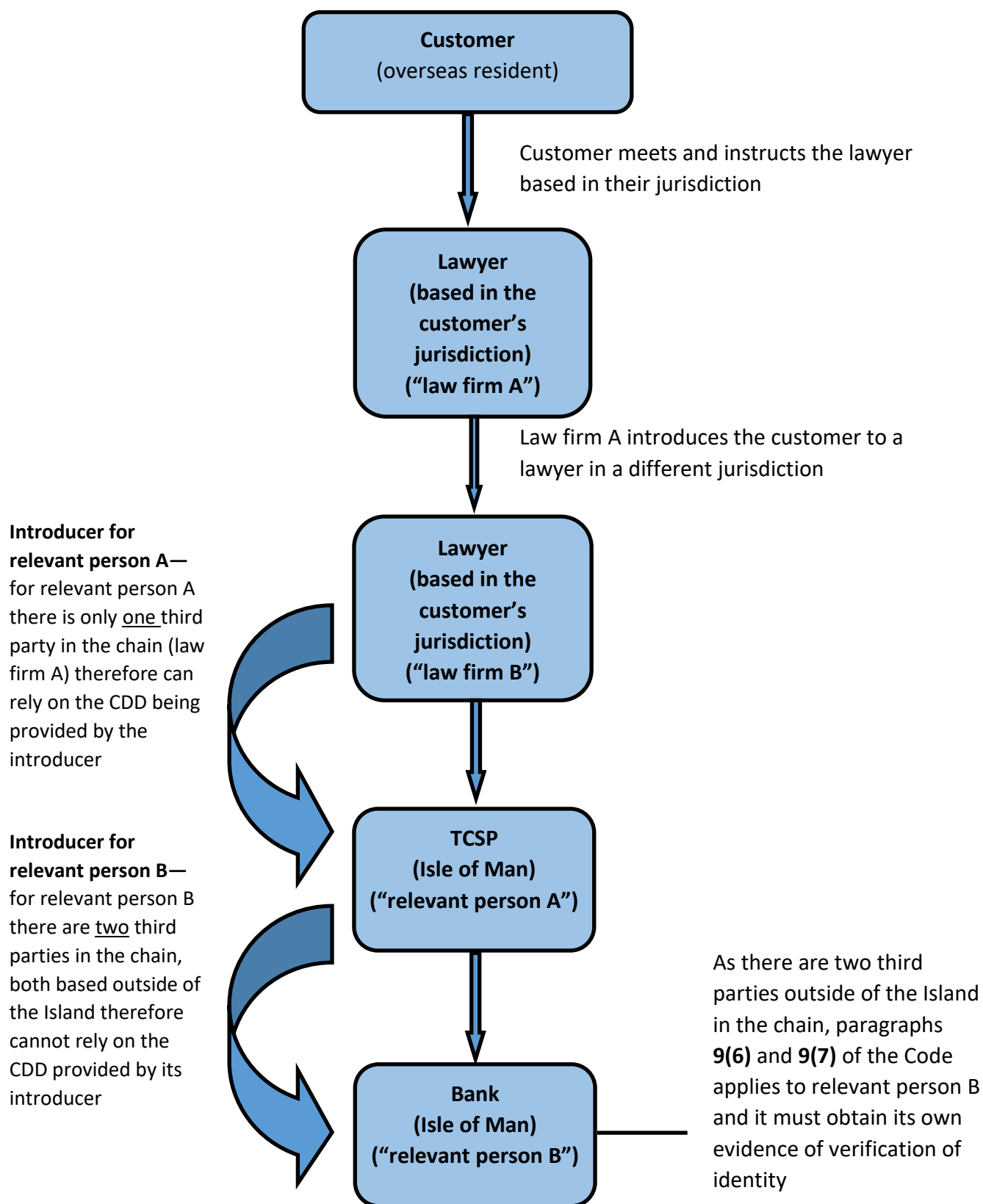
Law firm B is the introducer to relevant person A so there is only one third party in the chain, law firm A. Relevant person A may rely on the evidence of verification of identity provided by that entity (i.e. the provisions of sub paragraphs (6) and (7) do not apply).

Relevant person B, however, is in a different situation; its introducer is relevant person A and there are two third parties outside the Island, law firm A and law firm B. The provisions of sub paragraphs (6) and (7) therefore apply and relevant person B must make sure that it obtains evidence of verification of identity either:

- a) directly from the customer, or
- b) from relevant person A, but only if relevant person A has obtained it directly from the customer or from a third party (e.g. law firm who has met the customer, or
- c) directly from a third party (e.g. law firm A) who has met the customer.

For the avoidance of doubt, if relevant person B, or the introducer (relevant person A) decide to obtain the evidence of verification of identity directly from a third party who has met the customer, that third party could be law firm A, or another third party not previously involved in this introduction process. In this instance the relevant person would need to re-visit the risk assessment undertaken in relation to the involvement of third parties.

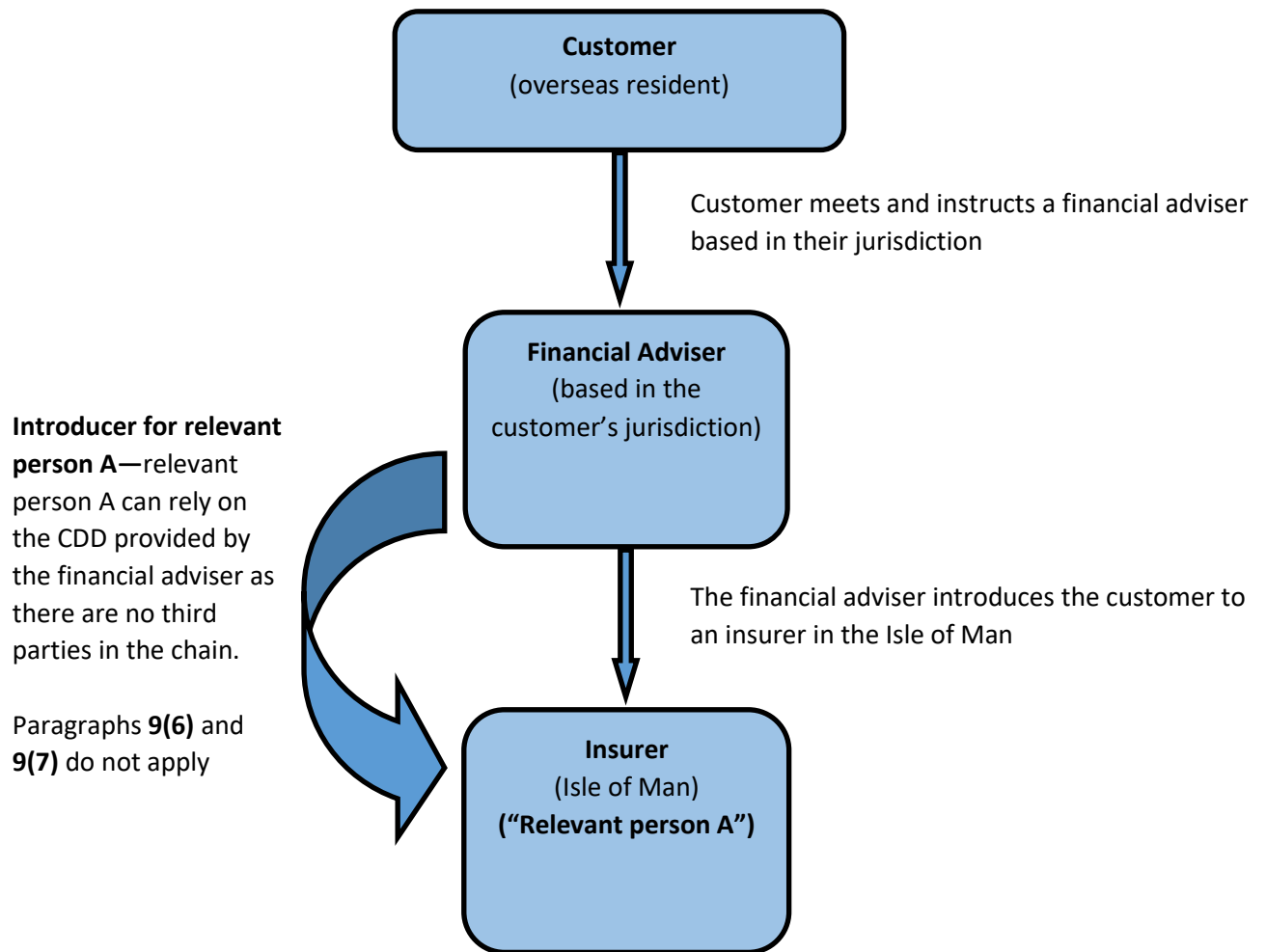
Scenario 3



#### **3.1.4 Scenario 4**

A customer who is an overseas resident meets and instructs a financial adviser based in their jurisdiction in relation to wishing to purchase an insurance product. The financial adviser introduces the customer to an insurer based in the Isle of Man (relevant person A). The insurer can rely on CDD and evidence of verification of identity provided by the financial adviser as the financial adviser is the introducer to relevant person A and there are no extra third parties in the chain.

**Scenario 4**



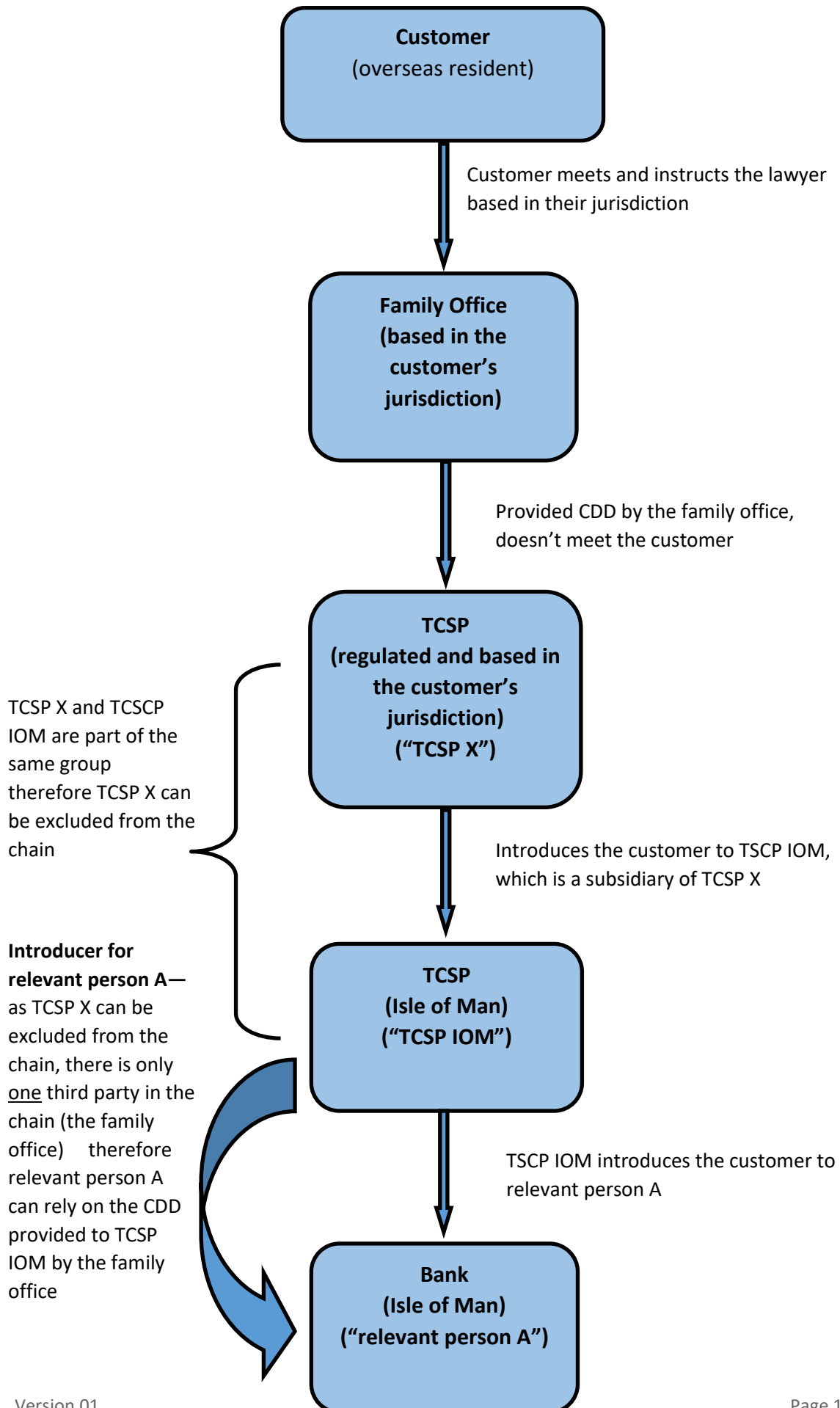
### 3.1.5 Scenario 5

The Family Office of a customer resident in jurisdiction X introduces its customer to a TCSP which is a regulated person in jurisdiction X (“TCSP X”). TCSP X does not meet the customer, but is provided with CDD and evidence of verification of identity by the Family Office. TCSP X then introduces the customer to a TCSP in the Isle of Man (“TCSP IOM”) which is a subsidiary of the TCSP in jurisdiction X. TCSP IOM then introduces the customer to a bank in the Isle of Man. The relevant person (for this example) is the bank in the Isle of Man.

The only person to have met the customer is the Family Office and there would initially appear to be two third parties (from the bank’s perspective) outside the Island (TCSP X and the Family Office) so one would normally expect the provisions of sub paragraphs 6 and 7 to apply. However, TCSP X and TCSP IOM are part of the same group and are both trusted persons, so TCSP X can be excluded from the chain.

In this scenario the introducer to the bank is TCSP IOM and the only third party is the Family Office. The bank in the Isle of Man can therefore rely on the evidence of verification of identity passed on to it by TCSP IOM and the additional provisions of sub paragraphs 6 and 7 do not apply.

**Scenario 5**



## 3.2 What information to verify

Code 8, 11,, 12, 15 It is a matter for relevant persons to decide what specific pieces of identity information to verify on a case by case basis relative to the materiality and risk of ML/FT with regard to their business, customer and technology risk assessments. The following are suggestions of the different pieces of identity information to verify for different types of customers.

### 3.2.1 Natural persons

In the case of natural persons, verification of identity could include:

- 1) Verification of identity information:
  - For all customers:
    - (i) name;
    - (ii) date of birth;
  - For standard and higher risk customers:
    - (iii) place of birth and / or nationality;
    - (iv) an official personal identification number; and
- 2) Verification of permanent residential address<sup>1</sup> (including postcode if possible).
- 3) Verification of identity and address of other persons per paragraph 12 of the Code.

### 3.2.2 Legal arrangements

In the case of legal arrangements, verification of identity could include:

- 1) Verification of identity information:
  - (i) name;
  - (ii) date of establishment;
  - (iii) official identification number; and
- 2) Verification of addresses:
  - (i) the mailing address(es) of trustee(s) (or other person controlling the applicant); and
- 3) Verification of the identity and address of other persons per paragraph 12 of the Code.

---

<sup>1</sup> If a different address is used for correspondence with a customer the relevant person should be comfortable in relation the rationale of using that correspondence address, and the validity of the address, particularly if sending any personal documentation to that address.

### 3.2.3 Foundations

In the case of foundations, verification of identity could include:

- 1) Verification of identity information:
  - (i) name;
  - (ii) date and country of establishment; and
  - (iii) official identification number.
- 2) Verification of addresses:
  - (i) address; and
  - (ii) address of the principal place of business where this is different to the registered office/business address.
- 3) Verification of the identity and address of other persons associated with the legal person per paragraph 12 of the Code.

### 3.2.4 Legal persons

In the case of legal persons, verification of identity could include:

- 1) Verification of identity information:
  - (i) name;
  - (ii) date and country of incorporation ; and
  - (iii) official identification number.
- 2) Verification of addresses:
  - (i) registered office address/business address; and
  - (ii) address of the principal place of business where this is different to the registered office/business address.
- 3) Verification of the identity and address of other persons associated with the legal person per paragraph 12 of the Code.

## 3.3 Examples of methods to verify identity and address

### 3.3.1 Example methods to verify the identity of a natural person

Code 8, 11,  
12, 15

The examples of methods to verify identity and address of customers, and other persons per Code paragraph 12, are not exhaustive, nor should they be considered limited. It may be that, according to the relevant person's circumstances and the results of their risk assessments, more information, documents or data is required to ensure they effectively manage and mitigate their ML/FT risks. Relevant persons should establish their own lists of the source documents, data and information they will accept in each case bearing in mind the principles and considerations set out in the Handbook.



Example method	Considerations
Passport	
National identity card	These forms of documentation do not always verify nationality or place of birth. Therefore care must be taken to ensure appropriate verification of nationality and / or place of birth takes place for the customer if required. A further document may need to be obtained from the customer to verify this information where it is deemed necessary as part of a risk based approach
Provisional or full driving licence	
Known employer ID card	
Proof of age card	
Birth certificates	
International driver's permits	<p>Caution should be exercised regarding International Driver's Permits/International Driver's Licenses. These can be obtained from unauthorised and unscrupulous operators on the internet who do not conduct any identification checks on the applicant for the Permit/Licence, and are marketed, for example, as a means of falsifying identity, avoiding driving fines and bans, and avoiding taking a driving test.</p> <p>International Driver's Permits can be genuine documents, but only when issued by competent national authorities to the holder of a valid domestic driving permit (i.e. national full driving licence) issued for use in the country of residence. The permit effectively converts a national licence into one for international use in other countries where the national licence is not recognised. An International Drivers' Permit is not a stand-alone document.</p>
The following additional checks may also be useful depending on the risk assessments:	
Require payment for the product or service to be drawn from an account in the customer's name at a regulated credit institution	
Independent data sources, including electronic sources	

### 3.3.2 Example methods to verify a natural person's address

Table 1 below sets out examples of the most reliable methods for verifying a natural person's address. Table 2 sets out other verification methods which may not, in isolation, provide the same level of confidence. Consideration should be given to whether the method used for verification provides suitable verification for all customers it is being provided for.

**Table 1: Most reliable address verification methods**

A recent account statement from a regulated bank, building society or credit card company
A recent mortgage statement from a regulated lender
A recent rates, council tax or utility bill (not including a mobile telephone bill)
Correspondence from an official independent source such as a central or local government department or agency in a List C jurisdiction
Photographic driving licence or national identity card containing their current residential address
The following additional checks may also be useful depending on the risk assessments:
<p>Make a physical validation by:</p> <ul style="list-style-type: none"> <li>• Making a telephone call to the customer with a telephone number that has been independently verified as belonging to the address in question; or</li> <li>• Sending a letter by registered post or courier to the address in question requiring the customer to respond with a signed confirmation of receipt or confirm to the relevant person a password or code contained in that letter.</li> </ul>

**Table 2: Other address verification methods**

Lawyer's confirmation of a property purchase or legal document recognising title to the property.
Tenancy agreement
Checking a phone directory
A letter from a known nursing home or residential home for the elderly confirming residence of the customer
A letter from a director or manager or a copy of a contract from a known Isle of Man employer that confirms residence at a stated address, and indicates the expected duration of employment. In the case of a seasonal worker, the worker's residential address in their country of origin should also be obtained and, if possible, verified
A letter from a person of sufficient seniority at a known university or college that confirms residence at stated address. The student's residential address in the Isle of Man should also be obtained
A letter from a director or manager (including a person from the HR Department) of a verified known employer that confirms residence at a stated address (or provides detailed directions to locate a place of residence) and expected duration of residence if known
A letter of introduction confirming residential address from a trusted person (as defined in the Code) addressed to the relevant person. The trusted person must be able to confirm they have obtained and verified, or re-verified the individual's address information recently

The following additional checks may also be useful depending on the risk assessments:
<p>Make a physical validation by:</p> <ul style="list-style-type: none"> <li>• Making a telephone call to the customer with a telephone number that has been independently verified as belonging to the address in question; or</li> <li>• sending a letter by registered post or courier to the address in question requiring the customer to respond with a signed confirmation of receipt or confirm to the relevant person a password or code contained in that letter.</li> </ul>
Independent data sources, including electronic sources.

### 3.3.3 Example methods to verify legal arrangements

This section sets out examples of methods to verify the identity and address of legal arrangements.

Trust Deed (or relevant extracts of the trust deed) and any subsequent deeds of appointment and retirement (or equivalent)
Bank statement (if applicable)
The following additional checks may also be useful depending on the risk assessments:
Require payment for the product or service to be drawn from an account in the customer's name at a regulated credit institution
Use independent data sources, including electronic sources
Consider obtaining sight of the letter of wishes, or other relevant documents of the trust, to confirm the beneficiaries / potential beneficiaries to the trust

### 3.3.4 Example methods to verify foundations

This section sets out examples of methods to verify the identity and address of foundations.

Foundation instrument (or relevant extracts of the foundation instrument)
Bank statement (of applicable)
The following additional checks may also be useful depending on the risk assessments:
Require payment for the product or service to be drawn from an account in the customer's name at a regulated credit institution
Independent data sources, including electronic sources

### 3.3.5 Example methods to verify legal persons

This section sets out examples of methods to verify the identity and address of legal persons.

Certificate of Incorporation Memorandum ( and / or Articles of Association) Equivalent document to the above (i.e. foundation charter)
Bank statement or utility bill
Latest Annual Return
Audited financial statements which displays the company name, directors and registered address
Prepared accounts by a reporting accountant which displays the company name, directors and registered address
Conducting and recording an enquiry by a business information service
An undertaking from a reputable and known firm of lawyers or accountants confirming the documents submitted
Undertaking a company registry search, including confirmation that the institution has not been, or is not in the process of being dissolved, struck off, wound up or terminated
The following additional checks may also be useful depending on the risk assessments:
Require payment for the product or service to be drawn from an account in the customer's name at a regulated credit institution
Independent data sources, including electronic sources

### 3.3.6 Example methods for verifying the natural persons with the power to direct a customer

Code 12 This section sets out examples of methods for verifying the identity of natural persons with the power to direct a customer. Not all information required to be obtained or verification needed may be provided by these documents. Consequently, relevant persons may choose to use the other methods such as the examples listed in previous sections.

Obtaining a copy of signatory lists
Latest annual return
Third party authority signing mandate
Register of directors/council members

## 3.4 Certification of hard copy documents

This section sets out some examples of suitable persons to certify documents who are generally viewed as known and trusted members of the community:

A member of the judiciary, a senior civil servant, a serving police or customs officer
--

An officer of an embassy, consulate or high commission of the country of issue of documentary verification of identity
A lawyer or notary public, who is a member of a recognised professional body
An accountant who is a member of a recognised professional body
A company secretary who is a member of a recognised professional body
A director, secretary or board member of a trusted person as defined in the Code
A manager or other senior officer within the relevant person's group

This list is not exhaustive and relevant persons can make their own risk based determination regarding who would be suitable to certify documents.

For the certification to have value in the CDD process, the certifier should sign and date the copy document (printing their name clearly in capitals underneath) and clearly indicate their position or capacity on it and provide contact details. If the document contains a photograph, the certifier should check the photograph represents a good likeness of the customer and should also state that it is a true copy of the original. There is no exact wording to use, however the relevant person should ensure it covers the aforementioned areas.

The certifier may complete a covering letter or document, which is then attached to the copy identification document(s) i.e. the certification is not written on the copy identification document itself. This is suitable as long as the covering document contains the information specified in the paragraph above, and it is clear in the letter itself that it refers to the attached document.

Relevant persons should ensure that any certified documents they have received are accurate and up-to-date and recently certified. Relevant persons should also consider the clarity and legibility of hard copy documents, including the clarity of security features such as holograms, stamps and watermarks.

### 3.5 Electronic methods to verify identity and address

The below table provides various methods relevant persons may wish to utilise in the verification of identity and address. This list is not exhaustive.

There are numerous factors a relevant person may consider when assessing the suitability, reliability, and integrity of the various methods which could be utilised to verify identity and address, many of which may be applicable across all the methods listed in the below table.

The Authority has identified these overall considerations as:

- comparison of a document to a genuine template document;
- legibility of key data on documents;
- clarity of image(s) / photograph(s);
- clarity of security features such as holograms, stamps, and watermarks;

- vulnerability to tampering of certain file types; and
- method of receipt and security of method, for example via email, or through an online portal.

<b>Method</b>	<b>Considerations</b>
Electronically certified identity / proof of address document	<ul style="list-style-type: none"> <li>• Must be certified using a secure electronic system</li> <li>• Relevant persons must satisfy themselves of the reliability and veracity of the system prior to accepting documents certified in this way</li> <li>• Certifier must have seen the hard copy document in order to certify the copy is a true copy of the original</li> <li>• Suitability of certifier</li> <li>• Affiliation / registration of system with a trust service or oversight provider e.g. eIDAS</li> <li>• Registration of system with local data protection regulator / information commissioner</li> </ul>
Scanned copy of a document certified in hard copy	Suitability of certifier
Photograph of individual holding their identity / proof of address document PLUS clear scanned copy of the document	<ul style="list-style-type: none"> <li>• Time stamp on photograph – current?</li> <li>• Clarity of photograph</li> <li>• Clarity of scanned copy of the document</li> <li>• Legibility of key data on photograph AND scanned copy</li> </ul>
Use of a software application (“app”)	<ul style="list-style-type: none"> <li>• Control of the image capture – i.e. whether this is controlled by the user or app</li> <li>• Control of the transmission process – i.e. whether this is controlled by the user or app</li> <li>• Dual authenticity to access the app / capture images / transmit (e.g. password, thumbprint)</li> <li>• Time restrictions on image capture – presence of the individual at the time the image is captured</li> </ul>

	<ul style="list-style-type: none"> <li>• Geotagging – is the individual in the expected location when accessing the app / capturing images / transmitting</li> <li>• Security of connection used to transmit images captured through the app</li> <li>• Video or micro-stream of photographs as a liveness check – presence of the individual at the time the image is captured</li> <li>• Affiliation / registration of app with a trust service or oversight provider e.g. eIDAS</li> <li>• Registration of app with local data protection regulator / information commissioner</li> </ul>
<p>Use of independent and electronic data sources</p>	<ul style="list-style-type: none"> <li>• Use of negative information sources (e.g. fraud, deceased individuals)</li> <li>• Use of alert data sources</li> <li>• Sources are required to be kept up to date</li> <li>• Affiliation / registration of provider with a trust service or oversight provider e.g. eIDAS</li> <li>• Registration of provider with local data protection regulator / information commissioner</li> </ul>

### 3.6 Methods for meeting a customer

Code 5, 6, 9, 15

One method of meeting a customer is for the customer to be physically present. However, in the digital age, being physically present is not necessarily the only method of meeting a customer.

A further method of meeting a customer can include (subject to the business, customer and technology risk assessments) the use of real-time visual communication media over the internet such as full-motion video conferencing. When using such media, the relevant person/introducer or other third party should clearly see the customer’s face and their image on the document used to verify identity (as per the relevant person’s procedures and controls) at the same time in order to be satisfied that the identity document belongs to the customer and the customer is who they claim to be.

A non-visual medium such as a telephone call does not qualify as meeting the customer.

## 4. Exemptions and simplified measures

There is no supplemental information associated with this chapter of the Handbook.

## 5. Reporting and registers

There is no supplemental information associated with this chapter of the Handbook.

## 6. Compliance and record keeping

Code 30 It is a matter for relevant persons to decide what must be included in the report required by paragraph 30(2) of the Code in order to cover the points listed. The following is a suggested list of points the periodic report may include:

### The AML/CFT environment (30(2)(a))

- changes made or proposed in respect of new AML/CFT legislation, regulatory requirements or guidance and actions that have been taken regarding these changes;
- other changes to the AML/CFT environment, for instance updates to the NRA, government enforcement actions or publications by competent authorities and details of any actions taken in relation to these;
- relevant persons who are part of a group may also wish to ensure that their senior management are made aware of any changes in respect of AML/CFT legislation and regulatory requirements and guidance which affect closely linked group companies and may have an impact on group requirements;
- changes or proposed changes to international standards or guidance in relation to AML/CFT and any actions that have been taken regarding those changes;
- the nature of actions taken by the relevant person in response to notices highlighting jurisdictions which are the subject of international countermeasures, and the measures taken to manage and monitor business relationships connected with such jurisdictions that have been highlighted as posing a higher risk of ML/FT;

### Internal developments (30(2)(b))

- the means by which the effectiveness of the relevant person's AML/CFT systems, controls and procedures have been managed and tested;
- the number of internal disclosures to the MLRO and the number of subsequent external disclosures submitted to the FIU, any perceived deficiencies in internal or external reporting procedures, and the nature of changes proposed or implemented to address any such deficiencies;



Activities relating to compliance with the Code (30(2)(c))

- information concerning the relevant person's AML/CFT training programme for the preceding year, which staff have received training, the methods of training and the nature of the training;
- information concerning the relevant person's procedures and controls for satisfying itself of the integrity of new staff members;
- any recommendations concerning additional resource requirements to ensure effective compliance with the relevant person's statutory and regulatory obligations;

Results of any testing undertaken (30(2)(d))

- any significant compliance deficiencies identified and details of action taken or proposed to address any such deficiencies; and
- details of any failures to apply the Isle of Man AML/CFT requirements in branches and subsidiaries and the proposed remediation of any such failures.

This list is not exhaustive or limited. Whilst this list is broadly grouped in relation to the requirements of sub-paragraphs 30(2)(a) – (d) of the Code some of the examples may be relevant to more than one sub-paragraph.

## **7. Miscellaneous**

There is no supplemental information associated with this chapter of the Handbook.